

ORIGINAL

## UNITED STATES DISTRICT COURT

for the  
Northern District of New York

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)LG Electronics, "Flip Phone", Black Color, Serial Number  
304CYTB062673, IMEI 013643-00-062673-1, Date 04/2013,  
Made in China, as further described in Attachment A

Case No. 5:19mj-462(ATB)

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location): LG Electronics, "Flip Phone", Black Color, Serial Number 304CYTB062673, IMEI 013643-00-062673-1, Date 04/2013, Made in China, as further described in Attachment A

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

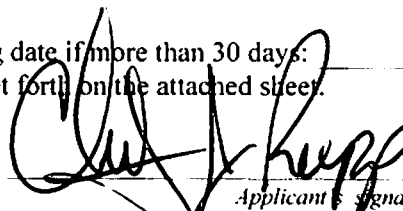
18 USC Section 2252A

Possession of Child Pornography

The application is based on these facts:  
See attached affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

 4300 HSI-SA

Applicant's signature

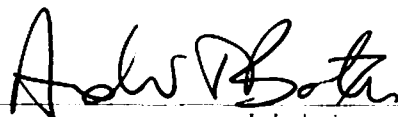
Christopher J. Rupp, Special Agent HSI

Printed name and title

Sworn to before me and signed in my presence.

Date:

7/23/2019



Judge's signature

City and state: Syracuse, New York

Hon. Andrew T. Baxter, U.S. Magistrate Judge

Printed name and title

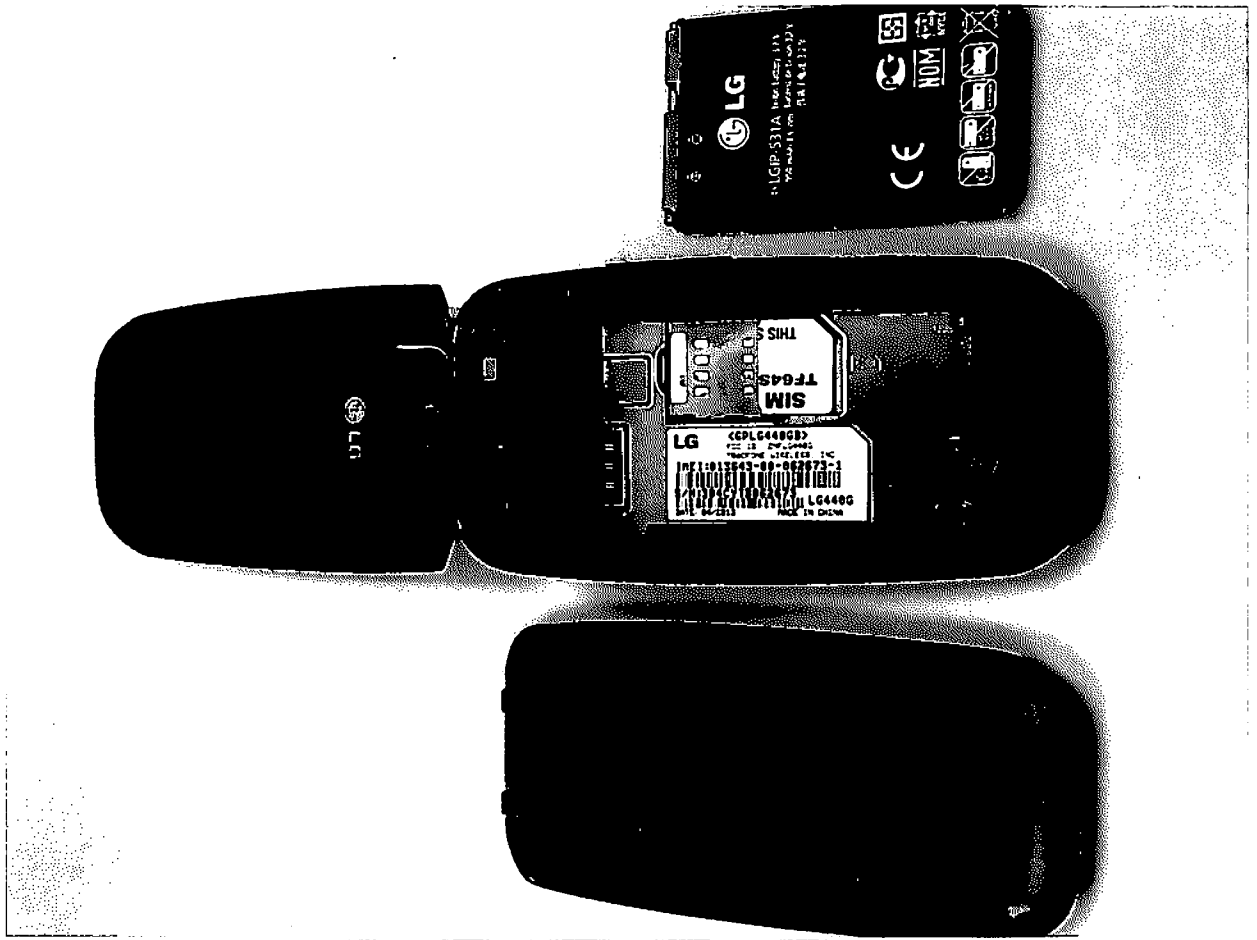
**ATTACHMENT A**

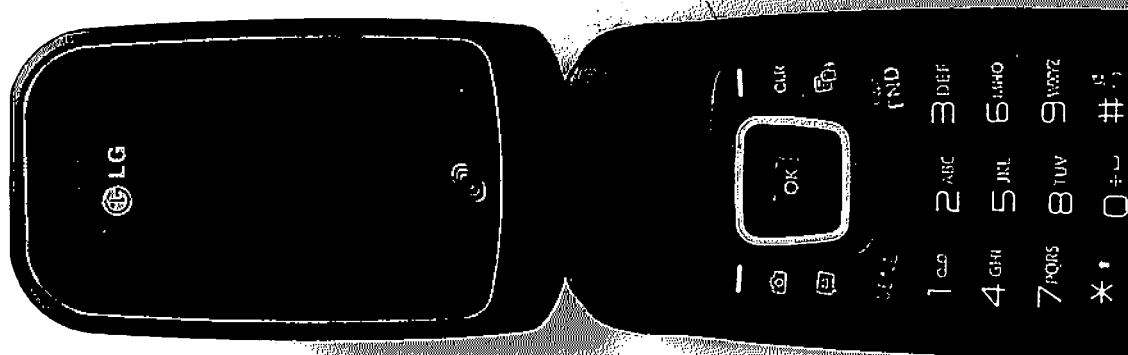
### DESCRIPTION OF THE SUBJECT ELECTRONIC DEVICE TO BE SEARCHED

The Subject Electronic Device is currently secured at the HSI Resident Agent in Charge Office Located in Massena, New York and is fully identified and described below as follows:

The Subject Electronic Device:

- LG Electronics, "Flip Phone", Black Color, Serial Number 304CYTB062673, IMEI 013643-00-062673-1, Date 04/2013, Made in China.





**ATTACHMENT B**  
**ITEMS TO BE SEARCHED FOR AND SEIZED FROM ITEM SUBJECT ELECTRONIC**  
**DEVICE**

- a. Items and information that constitute fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(5)(B) (possession of child pornography). Any and all visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
- b. Internet history including evidence of visits to websites that offer visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256.
- c. Correspondence or other documentation identifying persons transmitting through interstate or foreign commerce, including by mail or computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
- d. Computer records and evidence identifying who the particular user was who produced, downloaded or possessed any child pornography found on any computer or computer media.
- e. Correspondence and other matter pertaining to the production, purchase, possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in Title 18 United States Code, Section 2256, and evidence that would assist in identifying any victims of the above-referenced criminal offenses, including address books, names, and lists of names and addresses of minors, or other information pertinent to identifying any minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
- f. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, and notes evidencing an interest in unlawful sexual contact with children, and evidence assisting authorities in identifying any such children.
- g. Any and all records or communications with minor children, or with persons purporting to be minors.
- h. Any and all electronically stored records reflecting personal contact with minors.
- i. Any notes, writings or other evidence that would assist law enforcement in identifying victims of sexual exploitation, witnesses thereto, or other subjects that may have assisted, conspired, or agreed to participate in the sexual exploitation of children.

- j. Records showing the use or ownership of Internet accounts, including evidence of Internet user names, screen names or other Internet user identification.
- k. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
- l. Computer-related documentation that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- m. Computer passwords and data security devices, meaning any devices, programs, or data - - whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records.
- n. Documents and records regarding the ownership and/or possession of electronic media being searched.
- o. The authorization includes the search of the electronic media listed on the face of the warrant, for electronic data to include deleted data, remnant data and slack space.

---

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF NEW YORK**

---

**IN THE MATTER OF AN APPLICATION  
OF THE UNITED STATES OF AMERICA  
FOR SEARCH WARRANT FOR:**

**[SEE ATTACHMENTS A and B HEREIN]**

---

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

CHRISTOPHER J. RUPP, being duly sworn, deposes and states:

**INTRODUCTION**

1. I am a Special Agent (SA) with the U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI), and I am empowered by law to investigate and make arrest for offenses enumerated in Title 18, United States Code, Section 2252A.

2. I have been employed as an HSI Special Agent since June of 2004 and I am currently assigned to HSI's Resident Agent Office in Alexandria Bay, New York. While employed by HSI, I have been responsible for enforcing customs laws, immigration laws and federal criminal statutes of the United States. I have received training at the Federal Law Enforcement Training Center, where I successfully completed the Federal Law Enforcement Criminal Investigator Training Program and the Immigration and Customs Enforcement Agent Training School. My responsibilities as a SA with HSI include, but are not limited to, conducting investigations, executing arrest warrants, executing search warrants, collection of evidence, interviewing witnesses, use of force, firearms and other law enforcement related topics. I have been an HSI Special Agent for approximately 15 years and have investigated /or participated in investigations of child pornography, narcotics, counter proliferation, smuggling and immigrated related cases. My duties include the enforcement of federal criminal statutes involving the sexual exploitation of children, as codified in Title 18, United States Code, Sections 2251 through 2259. I have participated in

searches of premises and assisted in gathering of evidence by means of search warrant. I have received training in the area of the importation and distribution of child pornography and had the opportunity to observe and review numerous examples of child pornography in many forms of media including video and computer media.

3. I am currently investigating Daniel PASSERO and his knowing possession of child pornography using a means and facility of interstate and foreign commerce, and in and affecting such commerce, in violation of Title 18 United States Code, Section 2252A(a)(5)(B).

4. As will be demonstrated in this affidavit, there is probable cause to believe that evidence relating to violations of Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) will be located on PASSERO's LG cellular "flip Phone", Serial number 304CYTB062673, which is black in color, and made in China, with a date of 04/2013, hereafter, the "Subject Electronic Device," as more fully described in Attachment A. The Subject Electronic Device was taken into custody on or about September 26, 2013, by PASSERO's New York State Parole Officer, Officer Eric Rice. I submit this affidavit in support of a search warrant authorizing a search of the Subject Electronic Device for evidence of the crimes, as described in Attachment B, including evidence, fruits, and instrumentalities of the Subject Offenses and personally identifying information confirming the owner of the Subject Electronic Device. This affidavit and application are made under Fed. R. Crim. P. Rule 41 for authorization to search the subject electronic device.

5. The statements and facts set forth in this affidavit are based in part on information provided by New York State Police (NYSP) Investigator Darryl Bazan, his investigative reports, conversations with New York State Parole Officer Eric Rice, arrest reports involving PASSERO and parole reports provided by New York State Department of Corrections and Community Supervision, as well as, my own training and experience, and knowledge of the investigation of Daniel M. PASSERO thus far. Since this Affidavit is being submitted for the limited purposes of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts and circumstances that I believe are necessary to establish probable cause to believe evidence, fruits,

and instrumentalities of the violation of Title 18 United States Code, Section 2252A(a)(5)(B) are presently located on the Subject Electronic Device.

**DEFINITIONS**

6. The following definitions apply to this affidavit and Attachments A-B:
- a. “Child Erotica” means materials or other items that are sexually arousing to persons having a sexual interest or desire in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or body positions.
  - b. “Child Pornography” includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).
  - c. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. § 1030(e)(1).
  - d. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.
  - e. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.



- f. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware.
- g. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
- h. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP

assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

- i. "Minor" means any person under the age of 18 years. See 18 U.S.C. § 2256(1).
- j. "Sexually explicit conduct" applies to the visual depictions that involve the use of a minor, see 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, see 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated: (a) sexual intercourse (including genital-genital, anal-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. See 18 U.S.C. § 2256(2)(A).
- k. "Visual depictions" include undeveloped film and videotape, as well as data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- l. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli

drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device.

**BACKGROUND ON ELECTRONIC DEVICES AND CHILD PORNOGRAPHY**

7. Based on my knowledge, training, and experience, and the experience and training of other law enforcement agents and investigators with whom I have had discussions, I know that electronic devices, including cellular telephones serve different roles or functions with respect to possession of child pornography.

8. An electronic device's ability to store images in digital form makes the cellular telephone itself an ideal repository for child pornography. The size of the electronic storage media used in cellular telephones has grown tremendously within the last several years, and some cellular telephones can store literally thousands of images at very high resolution.

9. As with most digital technology, communications made from a cellular telephone are often saved or stored on that device's hard drive or memory card. Storing this information can be intentional, for example, by saving an e-mail as a file, or saving the location of a favorite website in "bookmarked" files. Digital information, however, can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, users' Internet activities generally leave traces that a trained digital forensic examiner often can recover, including evidence and other items that show whether a cellular telephone was sharing data files, and some of the data files that were uploaded, downloaded and transferred. Such information is often maintained indefinitely until overwritten by other data.

10. Modern technology in the past several years has transformed the cellular telephone from a simple mobile telephone device into a mobile mini-computer commonly referred to as a "smart phone" capable of Internet access through wireless internet connections as well as cellular telephone signals; built in digital camera and video camera capabilities are common features; video and image storage capabilities can hold thousands of images and hours of video files; and by being able to access the Internet virtually

anywhere, digital images and videos taken with a cellular telephone and stored on the cellular telephone can be shared with others by e-mail (phone to computer), text messaging (phone to phone), and uploaded to and displayed on Internet websites. Smart phones generally have global positioning satellite (GPS) capabilities that allow the cellular telephone to provide driving directions and include GPS coordinates in such features as sharing locations on social networking websites and imbedding into the metadata of photographic images the coordinates of where an image was taken.

### **COLLECTORS OF CHILD PORNOGRAPHY**

11. From my training and experience and based on information I have learned from other law enforcement officials and sources, I know the following:

12. Individuals who are interested in child pornography may want to keep the child pornography files they create or receive for additional viewing in the future. Individuals who collect child pornography may go to great lengths to conceal and protect from discovery their collections of illicit materials. They often maintain their collections in the privacy of their homes, on cellular telephones, or in other secure locations. Because the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished fantasies, the collector rarely, if ever, disposes of his collection. The collection may be culled and refined, but, over time, the size of the collection tends to increase. Individuals who utilize a collection in the seduction of children or to document that seduction treat the materials as prized possessions and are especially unlikely to part with them over time. Also, individuals who collect child pornography may search for and seek out other like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also may help these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to: text messages, video messages, electronic mail, email, bulletin boards, IRC, chat rooms, newsgroups, instant messaging, and other vehicles.

13. Individuals who collect child pornography may maintain stories, books, magazines,

newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals may keep these materials because of the psychological support they provide.

14. Individuals who collect child pornography may keep names, electronic mail addresses, cellular and telephone numbers, or lists of persons who have shared, advertised, or otherwise made known their interest in child pornography or sexual activity with minor children. These contacts may be maintained as a means of personal referral, exchange, and/or commercial profit. This information may be maintained in the original medium from which it was derived.

#### **BACKGROUND OF THE INVESTIGATION**

15. On or about July 24, 2010, Daniel M. PASSERO was residing with family members in Gloversville, New York when he was arrested and charged with sexual abuse of a minor under the age of nine years old. The victim was five years old at the time. PASSERO was ultimately convicted on November 30, 2010 of Sexual Abuse 1<sup>st</sup>, (sexual contact with an individual less than 11 years old), a violation of New York Penal Law Section 130.65 subsection 03. PASSERO was then incarcerated in state prison and deemed to be classified as a level three sex offender.

16. On or about July 19, 2013, PASSERO was released from state prison and placed on parole.

17. According to a NYSP report written by NYSP Investigator Darryl Bazan, on September 26, 2013, NYS Parole Officer Rice requested assistance from NYSP Mayfield Barracks with the forensic download of the Subject Electronic Device which Officer Rice seized from his parolee, Daniel PASSERO. Officer Rice stated that when he arrested PASSERO for an unrelated parole violation he left all of PASSERO's property with family members of PASSERO, who later contacted Officer Rice with concerns of digital images which had been found on the Subject Electronic Device. PASSERO stated that the photos were taken from a magazine called "Barely Legal" which he had access to through a friend. PASSERO advised law enforcement that he did not believe there were illegal photos on his Subject

Electronic Device, but he granted consent for the state police or parole to view his phone and retrieve any information on the phone. Inv. Bazan placed the Subject Electronic Device into evidence for later review at NYSP Troop G Computer Crimes Unit. The defendant was sent back to prison for violating parole (unrelated to the contents of the Subject Electronic Device) and was released again and placed back on parole on approximately May 18, 2015.

18. On October 30, 2013, Inv. Bazan completed a manual preview of the Subject Electronic Device since the Cellebrite forensic tool was unable to connect/communicate with PASSERO's Subject Electronic Device. Inv. Bazan advised that a manual search<sup>1</sup> of the Subject Electronic Device disclosed no evidence of a criminality was found on the phone<sup>2</sup>. At this point Inv. Bazan closed his investigation of the cellular phone and PASSERO and advised Officer Rice of his negative examination. The phone was returned to NYS Parole Officer Rice.

19. On or about April 27, 2015, a report was made to the NYSP regarding a then 14 year old female student who was enrolled at the Fonda-Fultonville High School, in Fonda, New York. The report in summation stated that a teacher found a letter written by the 14-year-old female student who claimed that while living in Gloversville, New York her mother's boyfriend had raped her while she was sleeping on the couch. The ensuing investigation of the matter by NYSP identified Daniel M. PASSERO as the likely individual who allegedly performed the sexual assault. The 14-year-old was confronted with the information contained in the letter and was interviewed at the Child Advocacy Center but denied any truth to the letter. According to NYSP Investigator Jones, the 14-year-old during his conversation with her denied the contents of the letter were true and became highly agitated by the conversation. On June 20, 2015, Inv. Jones visited the residence of PASSERO, 485 Frog City Road, Fort Plain, New York and attempted to interview PASSERO about the allegations in the above referenced letter. PASSERO admitted to knowing the 14 year-old female and stated that he did not remember what happened six years

---

<sup>1</sup> A manual search is not an analysis, but, merely the Investigator manually reviewing the phone. A Cellebrite tool provides a more thorough analysis.

<sup>2</sup> Inv. Bazan observed images of younger females, but they appeared to be legal to possess. No other images that appeared to be criminal or any other evidence of criminality was located during the manual preview.

ago (the 14 year-old female would have been approximately 8 years old) and did not want to further discuss the issue at hand and requested an attorney. The NYSP then closed the case due to lack of cooperation from both the victim and the suspect PASSERO. In preparation for this trial, the aforementioned child was re-interviewed by law enforcement. During the interview, she admitted that the PASSERO had, in fact, sexually assaulted her prior to her initial disclosure. Specifically, she advised law enforcement that PASSERO had performed oral sex on her.

20. On May 18, 2015 PASSERO was residing at 485 Frog City Road, Fort Plain, New York upon his release for the unspecified parole violation. While living at this address, PASSERO shared this residence with other family members and a family friend: his grandfather, Clarence Mushero; grandmother, Anne Mushero; aunt, Laurie Collins; uncle, John Collins; and a family friend, Scott Miller. On January 16, 2016, PASSERO's grandmother found a cellular telephone in residence's bathroom and told Scott Miller that she had found a phone she believed was his. Scott Miller examined the phone since it looked similar to a phone he had previously had lost, misplaced or had stolen from him while at the residence. Upon Miller's examination of the phone to determine ownership, Miller observed one or more sexually explicit images of minor children. Miller then turned the phone over to Clarence Mushero. Clarence Mushero confronted PASSERO about the phone and the images found and PASSERO admitted, in sum and substance, that he (PASSERO) had taken the phone and that he had accessed the Internet to get child pornography images. Clarence Mushero then contacted PASSERO's parole officer, Anthony Lucenti, requesting PASSERO be immediately removed from the residence.<sup>3</sup>

21. New York State Parole Officer Lucenti, along with a uniformed NYSP Trooper, responded to the residence to determine what transpired with PASSERO who was still on state parole. Upon arrival, Officer Lucenti was met by family members and spoke to Clarence Mushero and PASSERO. PASSERO told Officer Lucenti that he (PASSERO) took the phone from Scott Miller and that he was very sorry for downloading pornography and for lying to everyone. Officer Lucenti took

---

<sup>3</sup> Mr. Miller and Mr. Mushero were both previously arrested for sex offense crimes. Mr. Mushero was ultimately convicted of misdemeanor sexual misconduct in 1983, and Mr. Miller was convicted of misdemeanor harassment in 1996.



custody of the cell phone, confirmed the existence of child exploitative material on the phone and took PASSERO into custody for violating the terms of his parole. As a condition of his parole, PASSERO was not allowed to use, own or possess a computer/communication device and or internet capable device.

22. Officer Lucenti turned the cellular phone over to the NYSP who later conducted an initial forensic preview of the phone which disclosed child pornography. Additionally, on January 19, 2016 PASSERO was interviewed by NYSP Investigator Spato, as witnessed by Parole Officer Lucenti, and gave a written statement as to his (PASSERO's) use of the LG cellular smart phone to access the Internet and use Google to find images and websites of young girls. He also admitted his unauthorized taking and use of the LG cellular phone and that the phone contained child pornography.

23. On or about January 27, 2017 your affiant began a criminal investigation of PASSERO for his possession of child pornography relating to the LG cellular phone seized in January 2016. On this date, your affiant also took custody of the above-mentioned phone and retained such phone as evidence for criminal prosecution. On January 30, 2018 your affiant submitted LG smart phone to the NYSP's computer forensics lab in Albany, New York for advanced computer forensics. This advanced computer forensics disclosed the existence of hundreds of images of child pornography and erotica which were located on a "microSD card" which was inserted into the LG cellular smart phone PASSERO possessed.

24. On June 27, 2019, Your Affiant contacted Parole Officer Rice and spoke with Officer Rice regarding his 2013 interaction (above referenced paragraphs 16, 17 and 18) with PASSERO and the Subject Cellular Device PASSERO possessed at that time. Officer Rice advised he believed the phone was never returned to PASSERO. Office Rice made notification to PASSERO's mother to pick up the phone but neither she nor PASSERO ever came by to retrieve the Subject Cellular Device. Your Affiant asked Officer Rice if he would be able to locate the Subject Cellular Device, and Officer Rice advised he would look for the phone as he may still possess it in a box of abandoned items he retains. Officer Rice subsequently advised Your Affiant that he still retained possession of the phone as it was located in the abandonment box. Officer Rice then advised Your Affiant that he would be willing to turn the phone over to HSI. On Friday, June 28, 2019 HSI Special Agent Bowdy of HSI Albany, New York took



possession of the Subject Cellular Device and forwarded the phone via FedEx to Your Affiant. The phone is described as a black colored, LG brand, “flip” style phone with the following identifiers located on the inside of the phone: S/N:304CYTB062673, IMEI:013643-00-062673-1 and date of 04/2013.

25. On July 1, 2019, this Affiant received the above Subject Electronic Device as evidence in furtherance of the investigation of Daniel M. PASSERO.

26. At the time of the initial attempt by Inv. Bazan to analyze the phone in 2013, the device was not compatible with Cellebrite analysis. Your Affiant has been informed that current technology will now likely allow for a more in-depth analysis of the Subject Electronic Device.

27. Therefore, based on the information as described above including: PASSERO’s history of sexual offenses against minors, that a limited manual search of the Subject Device found “Barely Legal” sexual explicit adult pornography on the Subject Electronic Device and, that, less than three years after the limited search of the Subject Electronic Device, Passero was found in possession of child pornography on an LG cellular smart phone which he admitted to taking and using the Internet to obtain such images, Your Affiant asserts that there is probable cause to believe evidence, fruits, and instrumentalities of a violation or violations of Title 18 United States Code, Section 2252A(a)(5)(B) are presently located on the Subject Electronic Device

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

28. Your Affiant is familiar with electronic evidence recovery and, further, has spoken with law enforcement investigators trained in computer and cellular telephone evidence recovery that have extensive knowledge about the operation of cellular telephones and computer systems including the correct procedures for the seizure and analysis of these systems.

29. Based on my knowledge, training, and experience, and the information learned from law enforcement sources and elsewhere, your Affiant is aware that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, transferred, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost to the user. Even when files have been deleted, they can be recovered

months or years later using specialized forensic tools. This is so because when a person “deletes” a file on a computer or cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

30. Therefore, deleted files or remnants of deleted files may reside in free space or slack space—that is, in space located on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data or process in a “swap” or “recovery” file.

31. Apart from user-generated files, an electronic device may contain electronic evidence of it was used, what it was used for, and more importantly, who used it recently and in the past. This evidence can take the form of operating system configurations, artifacts from operating system or different application operation, file system data structures, and the virtual memory “swap” or paging files. Similarly, files viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache” located on the computer. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

32. Although some of the information called for by this search warrant might be found in the form of user-generated documents (such as photographic images and video files), smart phone style cellular telephones can contain other forms of electronic evidence as well:

- a. Forensic evidence of how the Subject Electronic Device was used, the purpose of its use, who used it, and when, is called for under this request for a search warrant. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Computer file systems can record information

about the dates and times files were created and the sequence in which they were created.

- b. Forensic evidence on an electronic device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence or physical location. For example, registry information, configuration files, user profiles, e-mail address books, “chats,” instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates and times) may in and of themselves be evidence of who used or controlled the computer or storage medium at a relevant time in question.
- c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw logical conclusions about how it was used, the purpose of its use, who used it, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance with particularity a description of the records to be sought, evidence of this type often is not always data that can be merely reviewed by a review team and passed along to the case agents and investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the nature of the evidence described in Attachment B also falls within the scope of the search warrant.
- e. Searching storage media for the evidence described in the Attachment B may require a range of data analysis techniques. It is possible that the storage media

will contain files and information that are not called for by the search warrant. In rare cases, when circumstances permit, it is possible to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, it is possible, though rare, for a storage medium to be organized in a way where the location of all things called for by the search warrant is immediately apparent. In most cases, however, such techniques may not yield the evidence described in the search warrant. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. As explained above, because the search warrant calls for records of how the Subject Electronic Device was used, what it was used for, and who used it, it is likely that it will be necessary to thoroughly search the device to obtain evidence including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a search warrant, a search the Subject Electronic Device for the things described in this search warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this search warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

**SEARCH METHODOLOGY TO BE EMPLOYED: THE SUBJECT ELECTRONIC DEVICE**

33. The search procedure of electronic and digital data contained in cellular telephones, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in such cellular telephone and its memory storage device to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents and scanning storage areas;
- e. performing key word searches to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and
- f. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

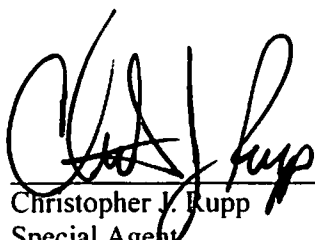
**CONCLUSION**

34. Based upon the above information, specifically the facts that:

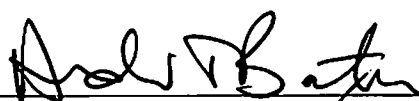
1. Passero is a convicted sex offender, having sexually abused a female less than 9 years of age;
2. Passero was previously found to be in possession of "Barely Legal" sexual explicit adult pornography on the Subject Electronic Device;

3. Passero was alleged to have sexually assaulted another female who was approximately 8-years-old at the time of the event;
4. In 2016, Passero was found in possession of child pornography on an LG cellular smart phone, which he admitted that he stole and that he used to obtain and/or view such images.

Your Affiant believes there is probable cause that evidence of violation of Title 18, United States Code, Sections 2252A(a)(5)(B) (possession of child pornography), as outlined in Attachment B of this Affidavit, will be found on the Subject Electronic Device that is the subject of this warrant as set forth in Attachment A. Therefore, based upon the information contained in this affidavit, your Affiant requests this Court issue the attached search warrant authorizing the search of the contents of the Subject Electronic Device set forth in Attachment A for the items more particularly described in Attachment B.

  
SA HSI  
#4300  
Christopher J. Rupp  
Special Agent  
Homeland Security Investigations (HSI)

Sworn to before me this 23rd day  
of July 2019.

  
HONORABLE ANDREW T. BAXTER  
UNITED STATES MAGISTRATE JUDGE  
NORTHERN DISTRICT OF NEW YORK

P

**ATTACHMENT A**

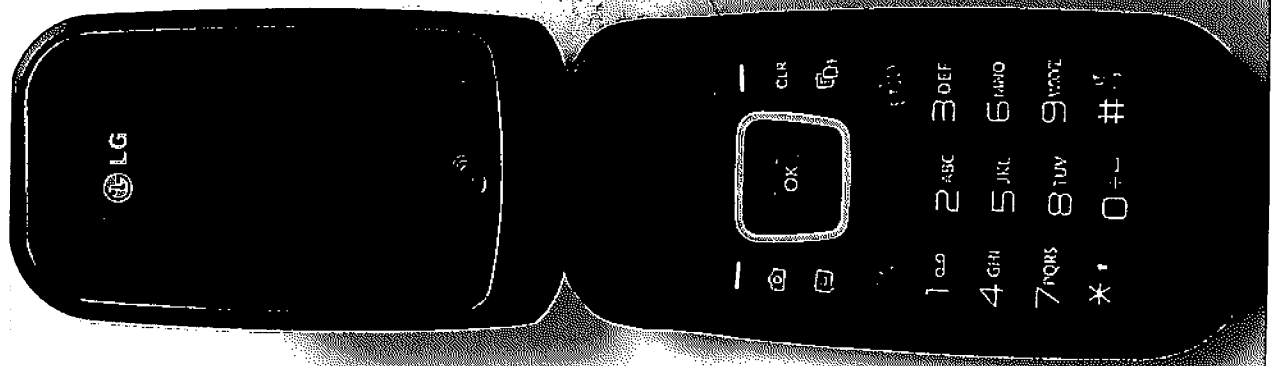
**DESCRIPTION OF THE SUBJECT ELECTRONIC DEVICE TO BE SEARCHED**

The Subject Electronic Device is currently secured at the HSI Resident Agent in Charge Office  
Located in Massena, New York, and is fully identified and described below as follows:

**The Subject Electronic Device:**

- LG Electronics, "Flip Phone", Black Color, Serial Number 304CYTB062673, IMEI 013643-00-062673-1, Date 04/2013, Made in China.







**ATTACHMENT B**  
**ITEMS TO BE SEARCHED FOR AND SEIZED FROM ITEM SUBJECT ELECTRONIC**  
**DEVICE**

- a. Items and information that constitute fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(5)(B) (possession of child pornography). Any and all visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
- b. Internet history including evidence of visits to websites that offer visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256.
- c. Correspondence or other documentation identifying persons transmitting through interstate or foreign commerce, including by mail or computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
- d. Computer records and evidence identifying who the particular user was who produced, downloaded or possessed any child pornography found on any computer or computer media.
- e. Correspondence and other matter pertaining to the production, purchase, possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in Title 18 United States Code, Section 2256, and evidence that would assist in identifying any victims of the above-referenced criminal offenses, including address books, names, and lists of names and addresses of minors, or other information pertinent to identifying any minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
- f. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, and notes evidencing an interest in unlawful sexual contact with children, and evidence assisting authorities in identifying any such children.
- g. Any and all records or communications with minor children, or with persons purporting to be minors.
- h. Any and all electronically stored records reflecting personal contact with minors.
- i. Any notes, writings or other evidence that would assist law enforcement in identifying victims of sexual exploitation, witnesses thereto, or other subjects that may have assisted, conspired, or agreed to participate in the sexual exploitation of children.

- j. Records showing the use or ownership of Internet accounts, including evidence of Internet user names, screen names or other Internet user identification.
- k. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
- l. Computer-related documentation that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- m. Computer passwords and data security devices, meaning any devices, programs, or data - - whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records.
- n. Documents and records regarding the ownership and/or possession of electronic media being searched.
- o. The authorization includes the search of the electronic media listed on the face of the warrant, for electronic data to include deleted data, remnant data and slack space.